REFINED PERMISSION CONSTRAINTS USING INTERNAL AND EXTERNAL DATA EXTRACTION IN A ROLE-BASED ACCESS CONTROL SYSTEM

BACKGROUND OF THE INVENTION

[**0001**] 1. Field of the Invention

[**0002**] The present invention relates to a system or method of Role Based Access Control (RBAC) for computer systems, which gains increased utility by enabling refined constraints on a role's access permissions at each request for access to an object. More particularly, permission constraints may be based upon the assessment of any or all of the subject, object, or environment information, which information may be gathered by data extraction from a variety of sources both internal to the controlled computer system and external to the controlled computer system, for evaluation relative to the constraints.

[**0003**] 2. Discussion of the Related Art

[**0004**] The technique of Role Based Access Control has greatly increased the utility of computer system access control. By pre-qualifying individuals, or subjects, in an organization into defined roles (e.g., doctor, head nurse, nurse) which are granted defined permission access to operate on the records, or objects; Role Based Access Control removes the necessity of developing defined access permission for each individual user to objects within the computer system. However, networked access to objects within the computer system, e.g., electronic data, has given rise to increased concerns for security, e.g., access to data such as proprietary information within an organizational structure or the privacy of medical records. Increasingly sophisticated demands are therefore being placed on the restriction of access to objects within the computer system, leading to a need for finer-grained access control than can be managed by traditional Role Based Access Control techniques that rely only on roles (and conditions on those roles; e.g., time constraints or location constraints) to establish permission for access to objects within the computer system.

[**0005**] After the RBAC model of Sandhu et al. in *Role Based Access Control Models*, publication number 0018-9162/96, IEEE, 1996, (hereinafter "Sandhu") several additional versions which limit role assignment, or which have increasing constraints on the granting of permissions were proposed, including: temporal and environmental limitations on role assignment. Some permission constraints have been proposed based on limited "context" evaluations such as Neumann et al., *An Approach to Engineer and Enforce Context Constraints in an RBAC Environment,* 2003, Association for Computing Machinery (ACM); and specialized content, such as Tzelepi et al., *A Flexible Content and Context-based Access Control Model for Multimedia Medical Image Database Systems,* 2001, ACM.

[**0006**] However, known RBAC systems have not been enabled to use context within all information categories, including and especially subject context. Further, known RBAC systems have not utilized entire categories of content since they have been limited to the controlled computer system. Thus, known RBAC systems have yet to enable system administrators to establish highly flexible constraints on a role's permission for dynamic granting of access to objects.

[**0007**] Thus, there is a need for an RBAC method which is enabled to gather information, i.e., seek and obtain data and compare such data to determine contexts necessary for the utilization of increasingly sophisticated constraints. There is a further need for access to be evaluated dynamically (i.e., at runtime, potentially changing throughout the duration of the session) based on constraints with respect to any or all combinations of subject information, object information, and environment information.

DEFINITIONS

[**0008**] "Access" is a specific type of interaction or operation between a subject and an object that results in the flow of information from one to the other, per Sandhu.

[**0009**] A "controlled computer system" denominates that electronic system in which the RBAC is installed in and therefore controls access to.

[**0010**] "Dynamically altered within a session" means that access can be altered and granted anytime before run time of the access grant, but without changing the assigned role.

[**0011**] "Each and every type or combination of" is used within the present application to mean that information is selectable from every category of information and from every combination of every category of information.

[**0012**] "Extracted information" is any information gathered or derived through the data retrieval or data extraction functionality of the present system, including but not limited to, text retrieval or term extraction from the requested objects or environmental content retrieved from outside the controlled computer system. It will thus be realized that the information extraction can be internal, i.e., within the controlled computer system, and external, i.e., outside of the controlled computer system, or both.

[**0013**] "Information" as used herein includes context, which is the relation of two or more data items, and content, which is the actual data.

[**0014**] "Object" is a passive entity that contains or receives information, per Sandhu.

[**0015**] "Subject" is an active entity, generally in the form of a person, process, or device, which causes information to flow among objects or changes the system state, per Sandhu, and as used herein is generally related to the user, including role assignment to the user. "User" may be thought of for explanatory purposes as a person who interacts directly with a controlled computer system, per Sandhu.

SUMMARY OF THE INVENTION

[**0016**] The present invention provides an RBAC method empowered to gather information, i.e., seek and obtain data and compare such data to determine contexts necessary for the utilization of increasingly sophisticated constraints. The present invention utilizes data extraction techniques to mine the wealth of content now available through larger networked sources, e.g., the Internet or any external databases accessible electronically either directly or indirectly by the controlled computer system. The present invention thus provides an RBAC method for the controlled computer system with sufficient content gathering or context analyzing capability, or both, to allow the use of easily formulated but refined constraints on permissions to access objects in an